DDoS or Distributed Denial of Service is a malicious attempt to disrupt the targeted server's normal traffic flow. It is an attack on the cybersecurity of a service or network. DDoS attacks are among the most widespread cyber attacks that immensely harm the system and make it go down for a long time.

## How Does a DDoS Attack Work?

The intruder intends to temporarily or permanently make the server or network unavailable to the user through a DDoS attack. They carry these attacks on networks that are Internet-connected machines. This internet is used to flood the targeted source with excessive requests.

### Use of Bots

Bots or zombies play an essential role in DDoS attacks to hinder cybersecurity. A group of bots is known as a botnet. When a hacker attacks a network, they use these bots or botnet to control it. Once a botnet is in place, the intruder or hacker can easily send remote instructions to each bot for a direct attack.

The bots send requests to the target IP address and flood their server. It becomes complicated to separate attack traffic from regular traffic because a bot is a legitimate internet device.

### Prominent Features of DDoS Attack

DDoS can render your cybersecurity easily because the artificial requests send from the attack come from multiple sources. Furthermore, these different sources reach your server at the same time. Thus, if you try to block a single source, it will not affect the other sources.

### Result of DDoS

A DDoS attack can be massive because artificial requests generate a large amount of traffic. It blocks your authentic users to use your network. Thus, if an organization does not deal with the problem in time then it can face a huge loss.

## An Analogy

To explain the working of DDoS to a layperson, let's consider an analogy:

The target system for our analogy is a shop. The attacker sends many people to the shop's door, which causes a blockage in the entrance. Thus, the real customers of the shop cannot enter now. It will result in a heavy loss for the shop because of which they will have to close temporarily (to fix the damage) or permanently (if the damage is too high).

## Conclusion

The most evident method to identify DDoS and enhance your cybersecurity is to check your network traffic and site working. If your site or server suddenly becomes slow, then it is a prominent symptom of DDoS.